FULL CONTENTS

[Claim(s)]
[Claim 1] A public key and the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, The encryption method characterized by having the step which memorizes the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, and the step which enciphers encryption object data using the public key of the above-mentioned lock data.
[Claim 2] The above-mentioned encryption object data is the encryption method according to claim 1 used as the decode key used for decoding the enciphered information.
[Claim 3] A public key and the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, The step which memorizes the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, The step which decodes one of the above-mentioned encryption common keys contained in the above-mentioned lock data with the secret key with which the above-mentioned group member corresponds, and generates the above-mentioned common key, The step which decodes the above-mentioned encryption secret key contained in the above-mentioned lock data using the common key which decoded [above-mentioned], and generates the above-mentioned secret key, The code decode method characterized by having the step which acquires the encryption object data enciphered with the above-mentioned public key, and the step which decodes the encryption object data enciphered [above-mentioned] using the secret key which decoded [above-mentioned].
[Claim 4] A public key and the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, The step which memorizes the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, The step which decodes one of the above-mentioned encryption common keys contained in the above-mentioned lock data with the secret key with which the above-mentioned group member corresponds, and generates the above-mentioned common key, The step which decodes the above-mentioned encryption secret key contained in the above-mentioned lock data using the common key which decoded [above-mentioned], and generates the above-mentioned secret key, The signature method characterized by having the step which memorizes the signature object data which performs a signature verifiable [with the above-mentioned public key], and to acquire, and the step which signs the above-mentioned signature object data using the secret key which decoded [above-mentioned].
[Claim 5] The step which acquires the public key and secret key which make a pair, and the step which acquires a common key, The step which enciphers the above-mentioned secret key with the above-mentioned common key, and generates an encryption secret key, The lock data generation method characterized by having the step which generates the encryption common key which enciphers the above-mentioned common key with each public key of a group member, and corresponds, and the step which generates lock data combining the above-mentioned public key, the above-mentioned encryption secret key, and the above-mentioned encryption common key.
[Claim 6] The step which acquires the public key and secret key which make a pair, and the step which acquires a common key, The step which transforms the above-mentioned secret key using the predetermined function with which an inverse function exists, and generates a deformation secret key, The step which enciphers the above-mentioned deformation secret key with the above-mentioned common key, and generates an encryption

deformation secret key, The lock data generation method characterized by having the step which generates the encryption common key which enciphers the above-mentioned common key with each public key of a group member, and corresponds, and the step which generates lock data combining the above-mentioned public key, the above-mentioned encryption deformation secret key, and the above-mentioned encryption common key.
[Claim 7] The step which acquires the public key and secret key which make a pair, and the step which acquires a common key, The step which enciphers the above-mentioned secret key with the above-mentioned common key, and generates an encryption secret key, The step which performs the function for redundant data generation to each public key of a group member, and generates redundant data, The step which generates the encryption common key which enciphers the group of the above-mentioned common key and the above-mentioned redundant data with each public key of the above-mentioned group member, and corresponds, The lock data generation method characterized by having the step which generates lock data combining the above-mentioned public key, the above-mentioned encryption secret key, and the above-mentioned encryption common key.
[Claim 8] A public key for the above-mentioned lock data to verify a signature and the secret key for an encryption signature which enciphered the secret key for a signature for performing the above-mentioned signature with the change authority owner's public key, The lock data generation method according to claim 5, 6, or 7 which includes further the signature by the above-mentioned secret key for a signature to the predetermined data contained in the above-mentioned lock data.
[Claim 9] The 1st public key and the encryption secret key which enciphered the secret key corresponding to the 1st public key of the above with the common key, Two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, The 2nd public key for verifying a signature, and the secret key for an encryption signature which enciphered the secret key for a signature for performing the above-mentioned signature with the change authority owner's public key, The step which memorizes the lock data which includes the performed signature using the above-mentioned secret key for a signature to the 1st public key of the above, the above-mentioned encryption secret key, the above-mentioned encryption common key, the 2nd public key of the above, and the above-mentioned secret key for an encryption signature, The step which decodes the above-mentioned secret key for an encryption signature contained in the above-mentioned lock data with the above-mentioned change authority owner's secret key, and generates the secret key for a signature, The lock data changing method characterized by having the step which changes the above-mentioned lock data, and the step which signs with the above-mentioned secret key for a signature to the changed lock data.
[Claim 10] The step to which the step which changes the above-mentioned lock data updates the 2nd public key of the above, [with the step which updates the above-mentioned secret key for a signature, and the new secret key for an encryption signature which enciphered with the above-mentioned change authority owner's public key, and newly generated the updated secret key for a signature] The lock data changing method according to claim 9 containing the step which updates the above-mentioned secret key for an encryption signature before change, and the step which signs with the secret key for a signature after renewal of the above.
[Claim 11] The above-mentioned lock data is the lock data changing method according to claim 9 or 10 of having the version identifier which shows the version of the above-mentioned lock data.
[Claim 12] The above-mentioned lock data is the lock data changing method according to claim 9, 10, or 11 which has a previous-version treatment identifier and controls the handling of the lock data of an earlier version based on this identifier.
[Claim 13] The above-mentioned previous-version treatment identifier is the lock data changing method according to claim 12 including the information which identifies the existence of the retrospective application of change of the above-mentioned lock data.
[Claim 14] The group lock containing a public key, the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, and two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member.
[Claim 15] A public key and the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, Encryption equipment characterized by having a means to memorize the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, and a means to encipher encryption object data using the public key of the above-mentioned lock data.
[Claim 16] A public key and the encryption secret key which enciphered the secret key corresponding to the

above-mentioned public key with the common key, A means to memorize the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, A means to decode one of the above-mentioned encryption common keys contained in the above-mentioned lock data with the secret key with which the above-mentioned group member corresponds, and to generate the above-mentioned common key, A means to decode the above-mentioned encryption secret key contained in the above-mentioned lock data using the common key which decoded [above-mentioned], and to generate the above-mentioned secret key, Code decode equipment characterized by having a means to acquire the encryption object data enciphered with the above-mentioned public key, and the means which decodes the encryption object data enciphered [above-mentioned] using the secret key which decoded [above-mentioned].
[Claim 17] A public key and the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, A means to memorize the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, A means to decode one of the above-mentioned encryption common keys contained in the above-mentioned lock data with the secret key with which the above-mentioned group member corresponds, and to generate the above-mentioned common key, A means to decode the above-mentioned encryption secret key contained in the above-mentioned lock data using the common key which decoded [above-mentioned], and to generate the above-mentioned secret key, Signature equipment characterized by having a means to memorize the signature object data which performs a signature verifiable [with the above-mentioned public key] and to acquire, and a means to sign the above-mentioned signature object data using the secret key which decoded [above-mentioned].
[Claim 18] A means to acquire the public key and secret key which make a pair, and a means to acquire a common key, A means to encipher the above-mentioned secret key with the above-mentioned common key, and to generate an encryption secret key, Lock data generation equipment characterized by having a means to generate the encryption common key which enciphers the above-mentioned common key with each public key of a group member, and corresponds, and a means to generate lock data combining the above-mentioned public key, the above-mentioned encryption secret key, and the above-mentioned encryption common key.
[Claim 19] The 1st public key and the encryption secret key which enciphered the secret key corresponding to the 1st public key of the above with the common key, Two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, The 2nd public key for verifying a signature, and the secret key for an encryption signature which enciphered the secret key for a signature for performing the above-mentioned signature with the change authority owner's public key, A means to memorize the lock data which includes the performed signature using the above-mentioned secret key for a signature to the 1st public key of the above, the above-mentioned encryption secret key, the above-mentioned encryption common key, the 2nd public key of the above, and the above-mentioned secret key for an encryption signature, Lock data changing equipment characterized by having a means to decode the above-mentioned secret key for an encryption signature contained in the above-mentioned lock data with the above-mentioned change authority owner's secret key, and to generate the secret key for a signature, a means to change the above-mentioned lock data, and a means to sign with the above-mentioned secret key for a signature to the changed lock data.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] The arbitrary members of a group enable it for this invention to perform decode and a signature about public-key-encryption technology using the group key which only a group member can use especially.
[0002]
[Description of the Prior Art] The cipher system called public key encryption is indicated in the U.S. Pat. No. 4,200,700 number. Public key encryption has the public key used when enciphering a plaintext, and the secret key used when decoding a code to a plaintext. A public key and a secret key are different keys, it is literally opened to the public and a public key can be set in the well-known state. Although the conventional cipher system (it is also called a secret key cipher, a common key code, and a conventional code) was a technical problem with important the same key being used for encryption and decode, and maintaining the confidentiality of a key, in this public key

cryptosystem, the confidentiality of the key of encryption becomes unnecessary. Moreover, when the number which communicates a cipher document is n man, an nx(n-1) /2 piece key is needed in it being the conventional encryption-decode common key system, but there is an advantage of ending with n keys, in a public key cryptosystem. Moreover, there is the feature that the same framework can be used also in a signature of everybody, i.e., the encryption processing by the secret key by everybody. For example, the cryptocommunication member P which has a secret key A changes Correspondence X with a secret key A, sends Document Y and Correspondence X which were changed to other members Q, and them [Member Q] If the conversion document Y is changed with the public key B of Member P and the conversion result of Y is in agreement with X, it can check that surely the document is sent by Member P. Thus, in a public key cryptosystem, it has the outstanding point of some which are not in the conventional cipher system.

[0003] Moreover, the composition about the assignment of a public key and a secret key to a group is indicated to JP,H7-297818,A. This is a system on condition of embedding a group secret key to the physical actual condition like a card, and the member of a group certainly possessing a card. That is, management of a key is realized using the physical actual condition of the card separated from the lasting existence of an individual by having composition using the actual condition of a card for the encryption system of an above-mentioned secret key and an above-mentioned public key.

[0004]

[Problem to be solved by the invention] In the public key cryptosystem, a lasting existence like an individual is set up as an independent unit. Therefore, sufficient function cannot be achieved when it is necessary to set up as one unit other than an individual (for example, two or more members). Moreover, it sets to the system which uses the above cards. The problem that judgment whether you are a just owner of a card, the problem, i.e., the card holder, of justification of the cardholder resulting from the problem of management of that hardware called a card must be used and the card itself, loss of a card, a theft, etc., is difficult occurs.

[0005] For example, like a company, organizations, such as the section, a section, or charge, are common work units, and are common work units which consist of two or more individuals who called it the task force realized independently of such an organization. Information also needs to be shared by the work unit common [these]. That is, in the relation between the interior of a common work unit, and the exterior, although it is necessary to maintain the confidentiality of information, circulation of the information between each internal member is needed. Therefore, the cipher system with which the arbitrary constituents of the common work unit can perform decoding processing to share information or signature processing is needed.

[0006] Furthermore, for the constituent of a common work unit, since change, such as an addition and deletion, may occur, a cipher system needs to be the method which can respond also to change of these constituents. In order [moreover,] to play a role like the chief of personnel administration in a company as well as a common work unit It is necessary to hold the specification and the continuous secret state according to the role in the form where it is independent of the specific individual who has played the role at a certain time, namely, can respond to change of the individual who has played the role.

[0007] This invention offers the cipher system which solves the above-mentioned problem. This invention presupposes that it is usable in the group which is the set which does not make an individual a unit for a public key cryptosystem, but uses an individual and a group as an element, and aims at offering the cipher system which the constituent (member) belonging to a specific group can decode.

[0008] Furthermore, this invention enables the signature by the arbitrary members belonging to a specific group, and aims at offering the signature method which can check that the signed document is the signature by the member belonging to the particular group.

[0009]

[Means for solving problem] In order to attain the above purpose according to this invention, it sets to the encryption method. A public key and the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, It is made to perform the step which memorizes the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, and the step which enciphers encryption object data using the public key of the above-mentioned lock data.

[0010] Since the cipher which enciphered the public key for encryption and the secret key corresponding to this with the common key, and the cipher which enciphered the above-mentioned common key with the group member's public key are included in lock data in this composition The group member can acquire a common key

using his own secret key, and can acquire the secret key which decodes with this common key further and decodes a cipher. By enciphering information with the public key of such lock data, it becomes possible to send information in the mode from which information does not leak other than a group member.

[0011] Moreover, in this composition, it can be considered as the decode key used for decoding the information enciphered in the above-mentioned encryption object data. For example, this decode key is used as a common key, and what is called a decode code scheme can be realized. That is, a common key is enciphered by a public key coincidence method using lock data, it sends to a group member, and a group member decodes this by lock data. And the cipher enciphered with the common key is decoded with the decoded common key.

[0012] Moreover, in order to attain the above-mentioned purpose according to this invention, it sets to the code decode method. A public key and the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, The step which memorizes the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, The step which decodes one of the above-mentioned encryption common keys contained in the above-mentioned lock data with the secret key with which the above-mentioned group member corresponds, and generates the above-mentioned common key, The step which decodes the above-mentioned encryption secret key contained in the above-mentioned lock data using the common key which decoded [above-mentioned], and generates the above-mentioned secret key, It is made to perform the step which acquires the encryption object data enciphered with the above-mentioned public key, and the step which decodes the encryption object data enciphered [above-mentioned] using the secret key which decoded [above-mentioned].

[0013] In this composition, the group member can acquire the secret key of lock data like ****. If it is a group member, the cipher simply enciphered with the public key of lock data also by whom can be decoded. And it cannot decode other than a group member. Moreover, in order to attain the above-mentioned purpose according to this invention, it sets to the signature method. A public key and the encryption secret key which enciphered the secret key corresponding to the above-mentioned public key with the common key, The step which memorizes the lock data containing two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, The step which decodes one of the above-mentioned encryption common keys contained in the above-mentioned lock data with the secret key with which the above-mentioned group member corresponds, and generates the above-mentioned common key, The step which decodes the above-mentioned encryption secret key contained in the above-mentioned lock data using the common key which decoded [above-mentioned], and generates the above-mentioned secret key, It is made to perform the step which memorizes the signature object data which performs a signature verifiable [with the above-mentioned public key] and to acquire, and the step which signs the above-mentioned signature object data using the secret key which decoded [above-mentioned].

[0014] Also in this composition, like ****, since it is only a group member, it can sign a group member by proving to data using this secret key that the secret key corresponding to the public key of lock data is acquirable. Those who acquired data with a signature can verify a signature using the public key of lock data.

[0015] Moreover, in order to attain the above-mentioned purpose according to this invention, it sets to the method of generating lock data. The step which acquires the public key and secret key which make a pair, and the step which acquires a common key, The step which enciphers the above-mentioned secret key with the above-mentioned common key, and generates an encryption secret key, It is made to perform the step which generates the encryption common key which enciphers the above-mentioned common key with each public key of a group member, and corresponds, and the step which generates lock data combining the above-mentioned public key, the above-mentioned encryption secret key, and the above-mentioned encryption common key.

[0016] In this composition, since the cipher of the secret key of the lock data which lock data enciphered with the group member's public key is included, the decode and signature of a cipher only by a group member are realizable. The above-mentioned secret key is transformed with the function (function with an inverse function) which is not tropism on the other hand about the above-mentioned secret key, and it enciphers with a common key and you may make it hold this deformation secret key in this composition. Moreover, when enciphering a common key with a group member's public key, you may use the function for seed generation. namely, -- calculating a group member's public key, predetermined function, for example, hash function, -- the value of this hash function, and the above-mentioned common key -- constructing (a predetermined operation, bit connection, etc.) -- it enciphers with the public key of the group member concerned. Since different seed for every public key of a group member will be added and the candidate for encryption will change if it does in this way, even if there are two or

more ciphers, it is rare to become the hint of decode.
[0017] Moreover, in this composition, said group member can be taken as either of the executives of a set of an individual and an individual, an organization, and an organization. Moreover, you may make it manage the above-mentioned lock data for the above-mentioned lock data as a unit. The user can use two or more lock data so that the bunch of a lock may be treated. A client can memorize the above-mentioned lock data to an accessible server.

[0018] Moreover, you may constitute the above-mentioned lock data so that the signature by the public key for verifying a signature, the secret key for an encryption signature which enciphered the secret key for a signature for performing the above-mentioned signature with the change authority owner's public key, and the above-mentioned secret key for a signature to the predetermined data contained in the above-mentioned lock data may be included further.
[0019] According to this invention, in the method of changing, lock data Moreover, the 1st public key, The encryption secret key which enciphered the secret key corresponding to the 1st public key of the above with the common key, Two or more encryption common keys which enciphered the above-mentioned common key with each public key of the group member, The 2nd public key for verifying a signature, and the secret key for an encryption signature which enciphered the secret key for a signature for performing the above-mentioned signature with the change authority owner's public key, The step which memorizes the lock data which includes the performed signature using the above-mentioned secret key for a signature to the 1st public key of the above, the above-mentioned encryption secret key, the above-mentioned encryption common key, the 2nd public key of the above, and the above-mentioned secret key for an encryption signature, It is made to perform the step which decodes the above-mentioned secret key for an encryption signature contained in the above-mentioned lock data with the above-mentioned change authority owner's secret key, and generates the secret key for a signature, the step which changes the above-mentioned lock data, and the step which signs with the above-mentioned secret key for a signature to the changed lock data.
[0020] In this composition, since only those who have change authority can acquire the secret key for a signature if those who generated lock data are removed, when a signature is verified by the success reverse side, it can check that those who have change authority have changed lock data about the lock data after change.
[0021] Moreover, the step which updates the 2nd public key of the above for the step which changes the above-mentioned lock data in this composition, [with the step which updates the above-mentioned secret key for a signature, and the new secret key for an encryption signature which enciphered with the above-mentioned change authority owner's public key, and newly generated the updated secret key for a signature] It can constitute so that the step which updates the above-mentioned secret key for an encryption signature before change, and the step which signs with the secret key for a signature after renewal of the above may be included. In this case, the change authority owner can set up a change authority owner by newly setting up the public key for a signature, and a secret key.
[0022] Moreover, the above-mentioned lock data may also contain the version identifier which shows the version of the above-mentioned lock data. Moreover, you may make it the above-mentioned lock data control the handling of the lock data of an earlier version based on this identifier including a previous-version treatment identifier. Moreover, the above-mentioned previous-version treatment identifier may be made to be generated based on the contents of change of the above-mentioned lock data. Moreover, the above-mentioned previous-version treatment identifier may also include the information which identifies the existence of the retrospective application of change of the above-mentioned lock data.
[0023] In addition, you may realize as hardware and this invention may constitute at least a part from a software realization mode. Moreover, when considering it as a software realization mode, it can install in computer system using communication media or a software package (record medium).
[0024]
[Mode for carrying out the invention] The outline of this invention is described first. In the following explanation, a set of an individual is called a group, and the individual who is the element of a group, i.e., a constituent, is called a member. This invention introduces the concept of a group in a public key cryptosystem. That is, it is the cipher system which considers the signature by the encryption which can decode the arbitrary members belonging to a specific group, and the arbitrary members belonging to a specific group as a typical function. In this invention, by enabling the signature by a group secret key, the member which actually signed is not clarified but it has the advantage that it can only be shown clearly that it is the signature by the member in a group.

[0025] The pair of the secret key corresponding to a group and a public key is offered, and each is called a group secret key and a group public key. Furthermore, the common key (conventional cryptographic key) which enciphers a group cipher key is offered. A group secret key is enciphered with a common key, this common key is enciphered with the individual public key of all the members, respectively, and a set of that enciphered common key is made. Each member makes available the group secret key which this enciphered common key gathered and enciphered at least. the arbitrary members in a group being able to decode by this the common key enciphered with the corresponding individual public key using their own individual secret key, and decoding a group secret key with this common key further -- that is, it can gain. Therefore, if arbitrary information is enciphered with a group public key, the member of a group can decode the enciphered information using the group secret key gained by the above-mentioned technique. Similarly the member of a group can sign using a group secret key.
[0026] Below, it clarifies about the processing in the case of change, such as generation of the pair of the group secret key which is needed in order to realize these functions, and a group public key, generation of a common key, encryption processing by a group public key, decoding processing by a group secret key and also an addition of the member of a group, and deletion.
[0027] When it is going to hold the confidentiality of information by encryption of information, the whereabouts of the enciphered information itself is not asked namely, clarified. It means being hard to accept the mechanism in which this must reencipher the once enciphered information for a certain Reason. It is because specification of the whereabouts of the information which must be reenciphered is difficult not to ask the whereabouts. therefore, in this invention, when there is change to the member which is the constituent of a group, the key instead of re-encryption of the enciphered information will once remake, and it will come out, and will correspond. With the public key cryptosystem which makes the conventional individual a unit, although the individual and key which are a lasting existence are one-body 1 correspondence and there was no request of remaking a key, in this invention, a correspondence relation called a group opposite key occurs, and the change request of a key based on change of the component of a group occurs.
[0028] The code and signature method of this invention have an effective function, also when it offers the key corresponding to the role of the chief of personnel administration in the individual in the position which plays the specific role of not only above-mentioned encryption and an above-mentioned signature of a group unit but an in-house, for example, a company. For example, there is a key corresponding to role of a chief of personnel administration, and when the individual who strives for a chief of personnel administration is changed, it can respond to change of the real world by changing the key corresponding to the role of a chief of personnel administration. The side which sends an encoded document to a chief of personnel administration should just encipher information using the public key corresponding to the role (chief of personnel administration) concerned from the former. Moreover, a new chief of personnel administration becomes possible [referring to the information enciphered in the past using the public key corresponding to the role concerned], without changing the already enciphered information.
[0029] In the group which has some purposes, such as a project in a company, the common work by two or more persons and the work based on a role are important, and neither the common WG's member nor the individual who plays a role is fixed. Therefore, what has the more advanced confidentiality retention capacity of the inside of a group and outside is required.
[0030] Moreover, although the system which gives the guarantee of a predetermined level to the public key called an authentication office in an information network services is being used, in this invention, exclusion of the key which became invalid is possible by using an authentication office.
[0031] Next, each element which constitutes this invention is explained. Explanation is given about the following items.
(1) The secret key (5) compound lock list (6) trust object (7) authentication office [0032] of a compound lock (2) group lock (3) individual lock (4) individual lock (1) A compound lock compound lock is a general term for the group lock (role lock) explained below and the lock which realizes an individual lock, and is electronic data which specifically has the following elements.
[0033] a. The human being who means the actual condition in the real world corresponding to a name compound lock is a legible character string, and has a role of an identifier of a compound lock. In order to prevent judging the character string from which man differs accidentally [be / the same], it is desirable not to carry out a space or use of a character string which is easy to be mixed up.
[0034] b. He is the maker of the date and time of creation, the time which created the maker compound lock, and

a compound lock. A maker performs the signature to the created whole compound lock. Enciphering the electronic data which constitutes a compound lock with a maker's personal key is included in the procedure of a signature.
c. The secret key of the secret key decode lock enciphered with the common key is enciphered with a common key.
[0035] d. It is a list, although the common key which enciphered the secret key of the list compound lock of a common key was enciphered with the public key of the member and the name (what is necessary is just data which identifies a member) of the member was given as a label. By decoding with the secret key of a member, a common key can be decoded, and, as a result, the secret key of a compound lock can be decoded and gained further. Decode of the code sent from others using the secret key of a compound lock is possible.
[0036] e. It is the public key of a public key compound lock. When enciphering information, with this public key, data conversion is performed and it is considered as a code.
[0037] f. The pair of a public key for the pair of the public key used for confidentiality maintenance of the secret lock list information of a change lock etc. and a secret key to control the right of change of a compound lock independently and a secret key is needed. This pair is called a change lock. The secret key of this change lock is enciphered with the public key of the right owner of change, and although the name of the right owner of change was given as a label, a compound lock holds a list. He is allowed only for the right owner of change of a compound lock to perform change of the compound lock, for example, the addition of a member, deletion, etc., and to create the compound lock of a high version. This right owner of change is specified beforehand. When a certain compound lock is changed by the right owner of change and becomes a high version, those who trust the lock of an earlier version can set up to trust the lock of a new version automatically. This is called an automatic trust mechanism. Trust of a lock is mentioned later. In order to clarify that a change of a compound lock was made by the just right owner of change, when changing, the signature by the secret key of a change lock is performed. However, when a compound lock's members of all the members have the right of change of the compound lock, the pair for security protections is used. In this case, the signature by the secret key of the present version is performed.
[0038] g. Public key above-mentioned the secret key and pair of a change lock of a change lock are constituted, it is used for decode of the signed compound lock by the secret key of the above-mentioned change lock etc., and the check of a signature is attained. In addition, the term of validity in the off-line period which can communicate with neither the term of validity of a compound lock nor an authentication office in addition to the above is added, and you may make it control use of a compound lock.
[0039] (2) A group lock group lock is a compound lock corresponding to the group in the real world. Generally a group contains two or more members. It functions also as a role lock (for example, role of a chief of personnel administration).
[0040] (3) An individual lock individual lock is a compound lock corresponding to an individual. An individual lock is also realized by the compound lock. The member of the compound lock as an individual lock specifies a depositor. It is the thing of the person by whom the conditionally same right as the individual was granted to men other than the individual with the depositor. This enables decode of information by making into a depositor those who can play a role of the individual's substitute person, when the individual has forgotten the path phrase. This takes into consideration the danger of entrusting the confidentiality and decode possibility of information in a company to one person's individual, for example. Moreover, it is also possible to use in order to perform audit and inspection of information. [0041] in which a setup that a depositor needs the approval of two or more specified depositors as conditions which can use an individual lock is also possible (4) The secret key of the secret key individual lock of an individual lock is protected so that only a user can access. For example, a secret key can be protected with the common key cryptography using the path phrase which only the individual (user) knows as a key of a code/decode. Or a user stores the secret key of an individual lock in always portable special instruments (an IC card, PDA: personal digital assistance etc.), and when required, you may make it take out. Moreover, the user's body / corporal features (a fingerprint, a voiceprint, a fundus-of-the-eye retina pattern, etc.) are detected, and you may enable it to access. You may use the feature detection by signature etc. In addition, the various access-control technique can be used. Thus, when only a user is needed in a secret key, he can obtain the secret key.
[0042] (5) It is a compound lock list with clear credibility which a compound lock list individual owns. A compound lock and its corresponding credibility are held as a pair. When using a compound lock, it is judged with the credibility under this list. It is interpreted as the credibility of the compound lock which does not exist here being unknown. For example, it is used, when specifying the individual or group which permits decode of a cipher by this compound lock list, acquiring that public key from a corresponding compound lock and generating an encryption

secret key. That is, the list of this compound lock is an open lock list which registered indirectly the public key of the individual who trusted it, or a group, and may register the public key of an individual or a group directly. In addition, the compound lock itself may refer to what was memorized by the equipment located in remoteness in addition to what was memorized by equipment, and the compound lock memorized in equipment and out of equipment may be intermingled for it and used for it.

[0043] (6) Although anyone can generate the compound lock used in the group in trust object this invention, unless it is trusted, it cannot change with an effective lock. It means as trusting it that the group (a role is included) which exists trusting a compound lock as the actual condition in the real world, and the compound lock which probably corresponds to the group actually correspond. A group and a compound lock not only must correspond, but specifically, the member of the group in the real world in the time of trusting it and the member contained in a compound lock must be in agreement. For example, suppose that there was a compound lock of the name "one Personnel Department personnel affairs." Although the group in the real world of the "Personnel Department personnel division" exists, the group in the real world of "one Personnel Department personnel affairs" may not exist. Even if the group in the real world of "one Personnel Department personnel affairs" exists, the just compound lock corresponding to it may not exist. Therefore, a compound lock cannot be trusted only for the name of a compound lock on a basis. Moreover, it cannot be trusted when the past member remains into the member of a compound lock, in spite of having changed the member in "one Personnel Department personnel affairs."

[0044] The information about the ability to be trusted [which compound lock] is called credit records. Moreover, the information which shows the credibility of the credit records themselves is also credit records. The subject holding credit records is called trust object. It is the arbitration of a trust object what is trusted for credit records and a compound lock as a basis. Two kinds of authentication offices explained to be individuals by following (7) exist in a trust object. The trust object can trust other trust objects. The trust object trusted at this time is called the body to be trusted. Only when the trust object trusts the compound lock, it will use this compound lock. It is trusted when the trust object currently trusted when a trust object does not have the direct credit records to the compound lock trusts the compound lock. Carrying out is possible.

[0045] For example, when an individual "Mr. Tanaka" and an authentication office "X business affairs" are all trust objects and the individual "Mr. Tanaka" trusts the authentication office "X business affairs", an individual "Mr. Tanaka" trusts automatically what the authentication office "X business affairs" trusts. However, an authentication office "X business affairs" does not necessarily trust what the individual "Mr. Tanaka" trusts conversely. It is the relation to say.

[0046] There is a kind of the grades of trust and it is called a trust level. It is possible to search for the credibility of the strange compound lock of credibility according to an operation using this trust level. The trust level used at this time is a trust level of the following tables, for example.

[0047]

[Table 1]

Level O: Trust it completely (ex. oneself).
Level O: Fully trust it.
Level **: Trust it to some extent.
Level ?: Unknown.
Level x: Don't trust it.

[0048] The example in the case of asking for the trust level to a compound lock with a strange trust level from the trust level to the compound lock which two independent different trust objects A and B over the same compound lock, for example, two persons' individuals, have is shown in drawing 1 . The 1st line of drawing 1 shows Individual A, a left end sequence shows Individual's B trust level, and the result about each case is shown as a table. For example, the trust level which Individual A set up is O, and the trust level which B set up? It comes out and the trust level of a certain compound lock becomes O.

[0049] Moreover, an algorithm as shown, for example in drawing 2 is used for the operation of a trust level which uses the trust level to a trust object, the trust level to other trust objects of the trust object, or the trust level to a compound lock. The 1st line of drawing 2 shows the trust level to a trust object, the trust level to the trust object of everything [sequence / left end] but the trust object, or the trust level to a compound lock, and the result about each case is shown as a table. For example, the trust level of the trust object is O, and the trust level which the trust object set up? It comes out and the trust level of a certain compound lock becomes ?. It is

possible to determine the credibility of a trust object with strange credibility or a compound lock using the algorithm shown by such drawing 1 or drawing 2 .

[0050] (7) An authentication office authentication office is one of the trust objects as mentioned above. The function which an authentication office offers is expressing and offering public trust in the unit of the company and organization where a certain encryption system is used, for example. The company and organization which manage the authentication office concerned determine arbitrarily the credit standard of the compound lock in an authentication office. Some methods [like] described below can be considered to the determination method of this credit standard. The act individuals other than a registrant prove it to be that the compound lock which is going to be registered in the following explanation saying "it guarantees" is just is said.

[0051] a) Check a just thing in a certain procedure by the specific manager of an authentication office. When a check is made, an authentication office trusts the compound lock. A certain procedure is the arbitrary procedure in the real world here. For example, it is based on the thumbmark's being stamped on an application form, or the check procedure of an applicant's identification card etc. In addition, it is trusted when it is more than the number the duplication check of a name, the guarantee by other specific individuals specified for every registrant, the guarantee more than the number decided beforehand, or the signature of the individual who trusts the authentication office was beforehand decided to be, and you may make it register.

[0052]

[Working example] The work example of the cipher system using a group lock is shown hereafter. In addition, although here takes up and explains the group lock in the compound lock in above-mentioned explanation, in the individual lock which is another kind of compound lock, the member in a group lock is changed into a depositor, and also a cipher system consists of same composition and procedure. Moreover, what is necessary is to set the number of configuration members of a group lock to 1, and just to consider it as the individual who has played the role now as the only member, in order to operate a group lock as a role lock although there is a role lock mentioned above as a use with a special group lock. However, employment of including the secretary else [a vice president's / own] in the member of a vice president's role lock is also possible.

[0053] The everybody using the cipher system of this invention have two lock lists. That is, they are "the open lock list" which is a list of a group lock and individual locks which a everybody trust, and the "secret lock list" which is a list of group locks by which b everybody can gain a secret key directly or indirectly based on an own secret key. Here, since it is easy, the group and individual lock which are contained in "the open lock list" assume that it is trusted, and it does not carry out giving trust of a degree the middle of "trusting it a little." Moreover, based on judgment of the thing or user for whom whether it is trusted or not used the algorithm about [above-mentioned] trust etc., detailed explanation in the following work examples is omitted. However, when a group lock is changed and the automatic trust mechanism in the case of trusting the last group lock, i.e., the group lock before change, is trusted, the group lock after change shall be trusted automatically. Moreover, although it cannot touch directly in the following work examples about the registration process to an above-mentioned authentication office, when an authentication office is all over a network like the explanation mentioned above, the registration to an authentication office is made about the lock generated or changed. However, this registration process is not the indispensable requirements for this invention.

[0054] First, drawing 3 explains the entire configuration of this work example. The fundamental function of this example is individual to individual, and is holding confidentiality correctly and transmitting information. However, the individual may belong to the group. The indirect method which minded file service also by the method of transmitting directly like e-mail may be used for transfer of information.

[0055] What is transmitted among individuals as shown in drawing 3 also transmits an individual public key and a group lock not only a code but if needed. When both an individual public key and a group lock need judgment whether it has the right correspondence relation with the individual and group to which it exists really in the real world, it is necessary to establish the judgment procedure.

[0056] In the case of the encryption to a code from the plaintext in the "individual" who shows drawing 3 , the lock corresponding to the lock by which self holds the individual who should make decode possible, and a group is chosen from a lock list, and it enciphers at it. The code which the selected individual and the individual belonging to the selected group can decode by this is generated. Or while enciphering a plaintext with a common key KA, the lock corresponding to the lock by which self holds the individual who should make possible decode of the decode key KB required for decode of this code, and a group is chosen from a lock list, it enciphers, and these are sent.

[0057] If direct decode with an own individual secret key is possible for the obtained code when decoding the

transmitted encryption information, it will decode using an own individual secret key. If decode by the group which belongs indirectly or directly is possible for self, a group secret key will be gained by changing a group lock into a group secret key using an own individual secret key, and it will decode using it. A group secret key is immediately thrown away after use, and if independent, it is not held. In this method, it is only an individual secret key that secret observance is demanded by the "individual." When encryption is performed by a common key KA, the decode key KB required for decode is first decoded using an own individual secret key. If decode by the group which belongs indirectly or directly is possible for self, a group secret key will be gained by changing a group lock into a group secret key using an own individual secret key, a decode key KB will be gained using it, and a plaintext will be decoded with this decode key KB.

[0058] [Group lock] The structure of the group lock in this example is shown in drawing 4 . Explanation of each sign in drawing 4 is shown below.

[0059] LG: It is the label string of this group lock. Duplication is not allowed in the lock list of some individuals. Since duplication may be produced as the whole, it does not carry out using as an identifier. However, since a public key is not in agreement, either, if a label is not in agreement, processing is accelerable using that.

[0060] PG: It is a public key according to the public-key-encryption system of this group lock which carries out public key use, and, generally is a 512 to about 2048-bit fixed-length data stream. When performing encryption which can be decoded to all the individuals who belong to this group directly or indirectly, it enciphers using this public key. Moreover, when checking what was signed as arbitrary individuals who belong to this group directly or indirectly, a signature is checked using this public key. in the group lock, the public key is contained in a form as it is -- anyone -- although -- it can be referred to.

[0061] SG: It is a secret key according to the public-key-encryption system of this group lock which carries out secret key use, and, generally is a 512 to about 2048-bit fixed-length data stream. It uses, when decoding the code enciphered with the corresponding public key. Moreover, also when signing as arbitrary individuals who belong to this group directly or indirectly, it uses. When this secret key is complexly enciphered by an individual secret key and an individual common key directly or indirectly and it uses, a common key is first decoded using an individual secret key, the secret key of a group lock is decoded and gained after that, after use is left immediately, and it does not carry out holding independently.

[0062] CG: It is the common key of the common key former which enciphers the secret key on a group, and DES, FEAL, etc. can use a well-known thing. Generally the size of a key is 128 bits from 40 bits.

[0063] CG (SG): It is the cipher which enciphered the secret key SG of the secret key group lock of the group lock enciphered with the common key CG with the common key CG. A common key CG is needed for acquiring a secret key SG.

[0064] Mi: It is the existence on the member concept of this group, and there is no direct expression in a data structure. An individual and a group can become a member. In addition, in the case of the individual lock instead of a group lock, this member becomes with a depositor as mentioned above.

[0065] PU: It is a public key according to the public-key-encryption system for this group lock change which carries out public key use, and, generally is a 512 to about 2048-bit fixed-length data stream. The group needs to make a change called an addition or deletion of a member. As a method of identifying people with the right that the change can be made, the pair of a public key and a secret key for exclusive use is used. This is the public key. It is enciphered directly or indirectly by the group lock with the individual secret key of the individual who owns the right of change, and the secret key for change is contained in it. When a group lock is changed, a new group lock is signed with the secret key for change. Since the secret key for change cannot be obtained if it is not the owner of the right of change, if the signature can be checked, it can check that it is change by the owner of the just right of change. This confirming processing can be automatically performed, if the former group lock is trusted. Since this public key for change is contained in a form as it is, anyone can refer to it.

[0066] SU: It is a secret key according to the public-key-encryption system for this group lock change which carries out secret key use, and, generally is a 512 to about 2048-bit fixed-length data stream. A function is as given in explanation of PU.

CU: It is the common key of the common key former which enciphers the secret key SU for group lock change, and DES, FEAL, etc. can use a well-known thing. Generally the size of a key is 128 bits from 40 bits.

CU (SU): It is the cipher which enciphered the secret key SU for the secret key group lock change for group lock change enciphered with the common key CU with the common key SU. A common key CU is needed for acquiring a secret key SU.

[0067] V: The version number of this group lock
It is the natural number. It is set to 1 when a group lock is generated newly. The version of a group lock is shown. the version from which the version number became criteria when changed -- 1 -- it is considered as many numbers.
[0068] F: Take one value of the value "needlessness" which shows the treatment of the last version, "necessity", and "deletion." When a group lock is changed, the individual with the last version needs to treat the last version appropriately by a high version coming to hand. "Needlessness" means that the last version becomes unnecessary. "Necessity" is required in order to check the signature made by the last version in order to decode the code made by the last version. In this case, when newly performing encryption and a signature, you have to use the newest version. Although "deletion" is close to "necessity", when self cannot gain the secret key of a high version, it means that the last version must be deleted. When a group lock is generated newly, this value does not have a meaning.
[0069] Ui -- it is the existence on the right owner concept of change of this group, and there is no direct expression in a data structure. An individual and a group can be specified as the right owner of change.
[0070] It is the label string of LMi:Mi. It is other group locks or the label of an individual public key which is the direct member of this group lock. Although not clearly written in this example about an individual lock, it consists of a secret key which a corresponding individual manages, and a public key to exhibit, and it is assumed that the label is given to the public key at least.
[0071] It is a public key according to the public-key-encryption system of PMi:Mi which carries out public key use, and, generally is a 512 to about 2048-bit fixed-length data stream. It is the public key of the direct member of this group.
[0072] PMi(CG): It is the result of enciphering CG by cipher processing according to the public-key-encryption system which was enciphered by PMi and which carries out CG use. In order to gain CG using this, the secret key SMi corresponding to PMi is required. This holds corresponding LMi by the array made into the index.
[0073] It is the label string of LUi:Ui. It is the label of the individual lock of the individual who is the right owner of change of this group lock.
[0074] It is a public key according to the public-key-encryption system of PUi:Ui which carries out public key use, and, generally is a 512 to about 2048-bit fixed-length data stream. It is the individual public key or the public key of a group lock which is the right owner of change of this group lock.
[0075] PUi(CU): It is the result of enciphering CU by cipher processing according to the public-key-encryption system which was enciphered with the public key of Ui and which carries out CU use. In order to gain CU using this, the secret key SUi corresponding to PUi is required. This holds corresponding LUi by the array made into the index. In addition, in this example, after adding the information for identifying data to a secret key like the data structure of the packet in packet communication, it enciphers. Therefore, when this encryption secret key is decoded, it can be distinguished easily whether based on additional information, the secret key was decoded normally.
[0076] Sig (SU): It is the data stream which shows the signature signature by SU to the whole. The whole is LG, PG, CG (SG), V, F, PU, CU (SU), LMi, PMi (CG), LUi, and PUi (CU) here. A signature is encryption processing by a secret key SU. In a public-key-encryption system, conversely, it can encipher with a secret key to usual and a contrary, and it can be decoded with a public key. Since it must encipher with a secret key in order to be able to decode with a public key, it can be checked by checking that it can decode with a public key that it has been signed with the secret key. In fact, a message digest is performed to the object range, and it signs with a secret key SU to the processing result. Since cost starts enciphering all the object ranges of a signature as a message digest, independently of the data size of the object range, it is the processing which generates about 128-bit information according to the contents of the object range. A message digest processing algorithm does not use a key using what was exhibited, either. Therefore, in the case of a check, the message digest of the object data will be carried out, and it will be checked whether it is in agreement with the result of having decoded the signature. Although processing of a message digest is processing similar to a checksum, it makes it difficult to forge the input data which generates the same result by on the other hand using a direction function in a processing process. Moreover, since the data size generated is large, forgery of round robin input data is also difficult. The name a "message digest" is a general name in code relation, and is the method learned well. Supposing Sig (SU) sets a message digest processing function to fmd, presupposes that an arithmetic sum expresses the combined control of the target data and expresses the signature using SU with Function SU, it will bring the result of having

performed the next processing.
[0077]
[Mathematical formula 1]
$$S_U\ (f_{md}\ (L_G+P_G+C_G\ (S_G)\ +P_U+C_U\ (S_U)$$
$$n$$
$$+\Sigma\ (L_{Mi}+P_{Mi}\ (S_G)\ +L_{Ui}+P_{Ui}\ (S_U)\ )\ )\ )$$
$$i=1$$

[0078] SU': It is a secret key according to the public-key-encryption system of the previous version which carries out SU use, and, generally is a 512 to about 2048-bit fixed-length data stream. It is the secret key for change of the last version. The function is the same as that of SU (for details, it is explanation reference of PU).
[0079] Sig (SU'): It is the data stream which shows the signature signature by SU' to the whole. The whole is LG, PG, CG (SG), V, F, PU, CU (SU), LMi, PMi (CG), LUi, PUi (CU), and Sig (SU) here. This is not given when created newly. When it is similarly written as Sig (SU), it can express as follows.
[0080]
[Mathematical formula 2]
$$S_U\ (f_{md}\ (L_G+P_G+C_G\ (S_G)\ +P_U+C_U\ (S_U)$$
$$n$$
$$+\Sigma\ (L_{Mi}+P_{Mi}\ (C_G)\ +L_{Ui}+P_{Ui}\ (C_U)\ +Sig\ (S_U)\ )\ )\ )$$
$$i=1$$

[0081] in addition, although it was made to sign to the whole data in this example, I want to prevent an alteration -- you may be made to sign to data in part.
[0082] [Open lock list] The structure of the open lock list in this example is shown in drawing 5 . Each individual owns an open lock list independently, and the group lock and individual lock which the individual trusts are held in the array which made the label of the lock the index.
[0083] The label of the group lock which Gi(s) : trusts the open lock list as shown in drawing 5 , and the LGi:group lock Gi, the individual public key of which Ii:trust is done, LIi: It consists of labels corresponding to the individual public key Ii.
[0084] Trust of a lock required in the case of addition of new data on an open lock list shall be left to judgment of the owner of an open lock list in this example. However, suppose that automatic trust of the following version of the group lock already trusted is performed. It is also possible to determine the lock or trust object which can be trusted using the algorithm about the above-mentioned trust level. In this case, it becomes possible to ask for a trust level certainly and easily by using the trust relation registered into the above-mentioned authentication office.
[0085] Although the group and individual of encryption who can decode in the case are specified, it is specified by choosing a corresponding group lock or a corresponding individual lock from one or more pieces and this open lock list.
[0086] When checking the justification of a signature, the public key corresponding to the secret key used at the time of a signature is picked out from this open lock list, and is used.
[0087] [Secret lock list] The structure of the secret lock list in this example is shown in drawing 6 . Each individual owns a secret lock list independently, and the group lock by which the individual can gain a secret key is held in the array which made the label of the group lock the index. Acquisition of a secret key is performed by applying the individual's individual secret key to a group lock directly or indirectly.
[0088] As shown in drawing 6 , a secret lock list consists of labels of the group lock which can use Gi:secret key, and the LGi:group lock Gi.
[0089] An addition on a secret lock list is performed by adding, if the group secret key inside the group lock can be gained by applying an own individual secret key directly or indirectly in the adding processing of the group lock to an open lock list. Therefore, the user does not need to be conscious of adding processing. Cautions are required, unless it becomes the basis which trusts the group lock with an own individual secret key just because it

can gain the group secret key inside the group lock.
[0090] In the case of decode, judgment of decode possibility is accelerated by using a secret lock list. Moreover, this secret lock list is used for acquisition processing of a required group secret key also in actual decoding processing.
[0091] Also besides using an own individual secret key, in the case of a signature, the group secret key under this secret lock list can be used, and it can be signed. If it does in this way, an informer's individual and group are discriminable by the sink side of a cipher. Moreover, if the public key of the secret lock used for the signature with the signature is attached, while the check of a signature will become easy, an informer can be easily checked only with a public key, without checking a signature.
[0092] [Code] The structure of the code in this example is shown in drawing 7 . In this example, decode is made possible by using either of two or more secret keys by giving the same structure as the list of pairs of LMi and PMi (SG) of a group lock. When this enciphers information to disclose to two or more persons, the necessity of not necessarily creating a group lock is abolished. That is, a sink's group which consists of an individual who chose from the open lock list arbitrarily, and a group can be created temporarily.
[0093] Each meaning of a sign in drawing 7 is explained below.
It is a public key according to the public-key-encryption system of the group lock which can be Pi(ed) : decoded, or the individual which carries out public key use, and, generally is a 512 to about 2048-bit fixed-length data stream.
[0094] It is the label string of Li:Pi.
[0095] D: Plaintext (information which should hold secrecy)
They are arbitrary data streams.
[0096] K: Since the common key public key encryption which enciphered Plaintext D has encryption processing and late decoding processing, it is common to adopt the hybrid system which enciphers a plaintext in a common key code and enciphers only the common key with public key encryption. This K is that common key. In this example, the decode by two or more groups or individuals is enabled by enciphering K by Pi, respectively.
[0097] Pi(K): D [0098] enciphered by **********KK(D): by Pi S: It is the secret key used when giving a signature to the secret key cipher which the person who performed encryption processing can use. One of an own individual secret key and the secret keys of the group lock contained in the secret lock list is used.
[0099] P: Use the public key corresponding to the secret key claimed that the signer used for the signature in the case of the check of the public key P signature which becomes the secret key S used for the signature, and a pair. Since the public key is specified, it holds. If the public key is contained in the own open lock list at the sink side of a cipher, it can check being signed by the group or individual whom self trusts, and the addresser or the sent group of a cipher can be checked.
[0100] Sig (S): It is the data stream which shows the signature signature by S to the whole. The whole is Li, Pi (K), and K (D) here. Refer to the clause of Sig (SU) of the structure of a group lock about a signature. If the same notation is followed, Sig (S) can be expressed as follows.
[0101]
[Mathematical formula 3]

$$S\ (f_{md}\ (\Sigma_{i=1}^{n}\ (Li + Pi\ (K))\ D))$$

[0102] [Flow of processing] The flow chart shown in drawing 16 from drawing 8 explains the flow of concrete processing of this example hereafter.
[0103] [Group lock generation] The flow about group lock generation is shown in drawing 8 . When creating a group (also in case of the same as when carrying out a current update), the maker needs to trust the group lock corresponding to the member specified newly, or the individual public key. Therefore, when not trusting the group lock of a member or the individual public key specified newly, in advance of creation of a group lock, you have to perform the addition to trusting it, i.e., a lock list.
[0104] The created group lock is first added to an own lock list. A lock list is a general term for an open lock list and a secret lock list. Furthermore, a required person (when decoding the code enciphered for the created groups, this group lock is required for the member of a group.) Conversely, a group lock is needed also when enciphering

for [this] groups. Arbitrary persons can perform encryption. therefore, distribution to those who may perform encryption for a member and these groups -- being needed -- it distributes. It is kept in the distant center, and a compound lock may be sent or you may make it send only the information which needs a compound lock if needed for the informer of a cipher, or a sink. Explanation of a distribution mechanism is omitted in this example.
[0105] The flow of drawing 8 is explained in detail. The label of the group lock first generated in Step 101 is inputted. It is examined by Step 102 whether the lock of the same label as the inputted label is already during a lock list. When creation of the lock of the overlapping label will be refused and already has the thing of the label same during a lock list, it progresses to Step 113 and creation of a group lock is stopped. When there is nothing of the same label, it progresses to Step 103.
[0106] At Step 103 and Step 104, Member Mi and the right owner Ui of change are specified. A member is a member using the encryption system which uses this group lock, and the right owners of change are those who have the right to perform change of this group lock, for example, the addition of a member, deletion, etc. Registration not only into an individual but a group is possible for each of members and right owners of change, and they chooses one or more group locks or an individual public key from the open lock lists which a group lock generation person has, and is specified.
[0107] At Step 105, the secret key SG, the public key PG, and common key CG of the group lock generated are generated. At Step 106, the generated secret key SG is enciphered with a common key CG, and CG (SG) is generated. Furthermore, PMi (CG) which enciphered this common key CG with each public key PMi of Member Mi is generated, and Label LMi is made to correspond to each.
[0108] At Step 107, the secret key SU for change of a group lock, the public key PU for change, and the common key CU for change to generate are generated. At Step 108, the generated secret key SU for group lock change is enciphered with a common key CU, and CU (SU) is generated. And a common key CU is enciphered with the public key PUi of the right owner of change, PUi (CU) is generated, and Label LUi is made to correspond to each.
[0109] The version number of the group lock generated is set up at Step 109. At Step 110, each data of LG, PG, CG (SG), PU, CU (SU), V and PMi (CG) which were generated at each step, and PUi (CU) is made into one. At Step 111, the signature by the secret key SU for change to united front data, i.e., data conversion, is performed. Generation of a group lock is completed by carrying out the registration addition of the group lock at Step 112 at the lock list of group lock generation persons. The generated group lock has the composition shown in drawing 4 explained previously.
[0110] [Addition on a lock list] The flow of an additional procedure to a lock list is shown in drawing 9 . An addition on a lock list is performed only about the public key of the group lock or individual who can trust it. This processing is used also in any of addition of the group lock which self generated and changed (creation of a high version), and addition of the group lock obtained from the others.
[0111] In this example, using the authentication office, a key is not distributed or the processing about distribution of being as distributing a key **** is not included through the E-mail or the floppy. Moreover, the signature to a key is used, reliability to the signer and credibility over a signer's key are calculated, and processing which computes the credibility of a key is omitted. It is possible to include acquisition of the credibility level by the operation of the credibility mentioned above into this flow, and to use for judgment of credibility. In this example, an automatic trust procedure of the version with a high group lock already trusted is shown. Here, only when a high version is able to check being signed with the secret key for change of the last version, it is trusted automatically.
[0112] An addition on a secret lock list adds only what can gain the secret key of the group lock directly or indirectly by using an own individual secret key out of the group lock currently trusted.
[0113] The flow shown in drawing 9 is explained in detail. If specification of the lock added at Step 201 is performed, it will set to Step 202,203,204. It is judged about the existence of the signature by secret key SU' for change of the lock of the last version, the existence of trust, and the accuracy of a signature, and when either is "no", the owner of a trust lock itself judges and inputs into Step 214 whether the lock progressed and added is trusted. When progressing to Step 210 when trusting it, and not trusting it, an addition on a lock list is not performed. The operation for acquiring the above-mentioned credibility in Steps 214 and 215 can be used.
[0114] Steps 205-209 are steps which opt for the treatment of a former version. When adding the group key of a high version, it is necessary to treat the group lock of a former version appropriately. This is judged with the value of F contained in the group key of a high version. Since a former version is old irrespective of the value of F, don't perform newly enciphering or signing. Therefore, you should divide the open lock list and the secret lock list with

the newest thing in addition to it. In this example, the classification was omitted, and when using, it is stopped for carrying out specification called the newest. The correspondence according to the value of F is as follows.
[0115] a) In F= "necessity", the group lock of an old version is left behind.
b) In F= "needlessness", the group lock of an old version is deleted.
c) In F= "deletion", it will be left behind if self can gain the secret key of a high version. Otherwise, it is deleted.
[0116] Steps 210-213 are steps which show that perform an addition on an open lock list and judge the availability of the secret key of the lock added, and an addition on a secret lock list is also combined, and it carries out when it can use.
[0117] [Availability judgment of a secret lock] The flow which judges the availability of a secret key to drawing 10 is shown. This is processing which judges whether the secret key which is enciphered and is contained in the specified arbitrary group locks can be gained by applying an own individual secret key directly or indirectly.
[0118] This processing uses a certain group lock for judgment (Step 212 and Step 213 of drawing 9) whether you may include in a secret lock list. In order to judge whether a group key can be used in the case of decode otherwise, the same judgment as this processing is required. However, [the group lock contained in the secret lock list] as far as it knows at the time Self can be managed with simple processing whether it is contained in the secret lock list, using being all the group locks which can gain a secret key in many cases, and must not use this processing directly in many cases.
[0119] The contents of processing judge whether the secret key of the group lock given first using an own individual secret key directly can be gained. Then, when it cannot gain, it is judged whether the secret key of the group lock given using each group key under own secret lock list directly can be gained. What is necessary is just to process in this procedure, if it only judges since it has become clear for the secret key of the group lock under secret lock list to be used.
[0120] The flow of drawing 10 is explained in detail. At Step 301, the group lock made into the object of judgment is specified, and it is examined by Step 302 whether an own individual lock is the member of the group lock which is a decision object, and if it is a member, it will be carried out [that it can use and]. When it is not a member, in Step 305, the element Gi of the present secret lock list is examined from Step 303, and it is examined whether Gi is the member of the key of a decision object. Step 303,304,305 means incrementing i of Gi one by one and performing it repeatedly. Among this repetition step, when one of Gi(s) is the members of the key of a decision object, it is judged that use is possible.
[0121] [Encryption] The encryption processing flow of information is shown in drawing 11 . What should be inputted here is the following three.
a) Specify the newest group lock contained in the person public presentation lock list which can be plaintext b decoded, or one or more individual public keys in all.
c) Specify only a signer's own individual secret key and the one newest group lock contained in a secret lock list. If it does not sign, it is not necessary to specify.
[0122] A signature is carrying out the message digest of the data which is a candidate for a signature, and signing the signature block which is the result with a secret key. The signature by a secret key is encryption by a secret key. About details, it is referring to the clause of Sig (SU) of a data structure "code" and a data structure "group lock."
[0123] The flow of drawing 11 is explained in detail. At Step 401, the information D holding secrecy is inputted and one or more public keys Pi corresponding to the newest group and newest individual who make decode possible at Step 402 are chosen from an own open lock list. This chooses the member which enables decode of the enciphered data.
[0124] At Step 403, a common key K is generated and encryption of the information D by the common key encryption system which uses K as a key is performed. It is because this has adopted the hybrid system which enciphers a plaintext in a common key code and enciphers only the common key with public key encryption since encryption processing and decoding processing of public key encryption are late as the column of the above-mentioned [code] described. In addition, this common key K may be the fixed thing which was what may not generate whenever it enciphers, and is generated if needed, or was decided beforehand.
[0125] At Step 404, K is enciphered with the public key Pi of each those who can be decoded, Pi (K) is generated, and the label corresponding to each is given. When not carrying out by judging whether the signature to the generated code is performed at Step 405, the conclusion of each data is performed at Step 410, and encryption processing is ended. When performing a signature, it progresses to Step 406.

[0126] Steps 406-409 are processing steps of a signature, and message digest processing (Step 406) of data in which it signs is performed. It is the processing which chooses the key for a signature from a secret lock list (Step 407), performs the signature by the selected secret key (Step 408), and packs array K (D) and a signed message digest (= signature block) (Step 409). Encryption processing is completed by the above step.
[0127] [Decode possibility judgment] The processing flow which judges whether self can decode arbitrary codes to drawing 12 is shown. This flow is used to, check which when listing a code file, is what can decode self for example. This flow is processing which performs judgment of decode possibility at high speed. It uses that it cannot specifically decode if a label is not in agreement, and coincidence of a label is checked first, when a label is in agreement, it restricts, and decode is tried. If the selection method of a label is generally decided appropriately, performance sufficient by this method will be obtained. There is also the method of accelerating by giving the open lock which cannot specify the selection method of a label and which was used not only for a label but for encryption at the "code" when becoming.
[0128] If the processing can try application of an own individual secret key and cannot decode it probably, it tries application of each group lock under own secret lock list. The decode in here is decode of Pi (K) corresponding to the label Li in a "code." Here, since it is not the purpose to obtain a plaintext, decode of K (D) is not performed.
[0129] The decode possibility judgment flow of drawing 12 is explained in detail. The code which judges decode possibility at Step 501 is specified. It is judged whether there is any coincidence with the label Li in a code and the label of an own individual lock at Steps 502 and 503. When there is coincidence, it progresses to Step 509 and decode is tried. When it cannot decode here, and when there is no label which is in agreement in Steps 502 and 503, coincidence with the secret lock label owned in Steps 504 and 505 is judged. When there is a label LGi in agreement, it progresses to Step 511, the secret key SGi of Gi corresponding to Label LGi is gained, and decode is tried at Step 512,513. When decode is not successful, it will progress to Step 506,507 and will investigate about the coincidence with the label of other possession secret lock lists, and coincidence with the label of an individual lock. In addition, it is shown that Step 506 repeats the same processing as Step 504 about a different label, and repeating Step 507 about a label which is different about Step 502 is shown. When it is able to decode in Step 510 or Step 513, judgment that it can decode at Step 514 is made.
[0130] [Acquisition of the secret key in a group lock] The flow which gains the secret key SG of the group lock which exists during a secret lock list at drawing 13 is shown. The secret key of a group lock is used in decode of code information, the case of a signature, etc.
[0131] Since only the group lock which can gain the secret key by applying an individual secret key directly or indirectly is contained in the secret lock list, it is clear that it can gain.
[0132] Processing tries to apply an own individual secret key directly first. When it goes wrong, it tries to apply the group lock under secret lock list. In the trial of application of a group lock, this processing is called recursively. The directed graph which makes a group a node and is formed considering the inclusive relation between groups called a member as an arc for ** does not have a loop. Therefore, a secret key can be gained by this processing.
[0133] The acquisition flow of the secret key SGi of drawing 13 is explained in detail. The group lock Gi under secret lock list is first specified at Step 601. When it is examined whether an own individual lock is contained in the member of the group lock Gi and it is contained at Step 602, it progresses to Step 607, PMi (CG) which enciphered the common key CG with the individual public key in the group lock Gi is extracted, this is decoded with an individual secret key, and a common key CG is gained. Furthermore, CG in a group lock (SG) is decoded with a common key CG, and the group secret key SG is gained.
[0134] In Step 602, when an own individual lock is not contained in the member of the group lock Gi, in Steps 603-605, it is examined to all the elements Gk of a secret lock list whether Gk is the member of Gi. This is a step which examines whether it is contained as a member of the group lock Gi about the "group locks Gk which can use a secret lock" of each which self holds. When Gk which is the member of the group lock Gi is detected at Step 604, the secret key SGk of Gk is gained at Step 608, enciphered PMj (SG) which is in the group lock Gi at Step 609 is extracted, this is decoded with a secret key SGk, and the group secret key SG is gained.
[0135] [Decode] The flow at the time of decoding arbitrary codes to drawing 14 is shown. The flow shown in drawing 14 is a flow almost equal to the "decode possibility judgment" processing mentioned above. Steps 701-713 are equivalent to Steps 501-513 in the decode possibility judgment flow of drawing 12 . However, in Step 714, using the key K of a common key code, K (D) is decoded and Plaintext D is gained. A signature is checked, while gaining Plaintext D if required when the signature is carried out to the cipher.
[0136] [Signature check] The flow of a signature check is shown in drawing 15 . The result of having performed

message digest processing to the candidate for a signature, and a signature block (data given by signature processing) are compared with the result decoded with the public key corresponding to the secret key it is supposed that was used on the occasion of a signature. If the two results are equal, a signature will be made correctly, and it can check that the candidate for a signature is not altered.

[0137] However, you have to trust the public key corresponding to the secret key used for the signature. What is necessary is to just be contained in the own open lock list. The check of a signature cannot be performed if it is not trusted.

[0138] When the result of a message digest and the decoded result are not equal, it turns out that the candidate for a signature is altered.

[0139] The signature check flow shown in drawing 15 is explained. At Step 801, the message digest of the candidate for a signature is carried out first. Since cost starts enciphering all the object ranges of a signature as a message digest as mentioned above, it is the processing which generates about 128-bit information according to the contents of the object range independently of the data size of the object range. Next, in Step 802, it judges about trust of the public key corresponding to the secret key used for a signature. When the public key is not trusted, it is judged at Step 806 that a signature check is impossible.

[0140] In Step 802, if the credibility of a public key is checked, it will progress to Step 803, a signature block will be decoded with the public key corresponding to the secret key it is supposed that was used on the occasion of a signature, and the identity judgment with a message digest will be made at Step 804. This actually serves as upper signature confirmation step. If it is judged that there is no identity in this step 804, in Step 807, a signature is not right. That is, it is judged that the secret key which signed is not right. If it is judged that a message digest and a decoded result are equal in Step 804, it will be concluded that the signature was justly performed in Step 805.

[0141] [Group lock change] The change flow of a group lock is shown in drawing 16 . There are the following four kinds of change of a group lock. The sequence from the left-hand side of the portion which has branched to processing of four shows a flow chart.

[0142] A. from now on -- an addition -- newly add a member. The added new member cannot decode the code enciphered before the addition. In this case, the pair of a new secret key and a public key is set to SG and PG of the group lock of a high version. Moreover, "it is for the value of F" necessary. Therefore, the individual who received a high version does not delete a former version. This is because it is required in order that the member from before may decode the code enciphered before the addition.

[0143] B. going back -- an addition -- newly add a member. The added new member can also decode the code enciphered before the addition. In this case, former SG and former PG are used as it is. Therefore, the value of F serves as "needlessness." Therefore, the individual who received a high version deletes a former version. What is necessary is just to use a high version, also when decoding the code enciphered before.

[0144] C. From now on, delete the member of deletion existing. The deleted member can decode the code enciphered before deletion. Naturally what was enciphered after deletion cannot be decoded. In this case, the pair of a new secret key and a public key is set to SG and PG of the group lock of a high version. Moreover, "it is for the value of F" necessary. Therefore, the individual who received a high version does not delete a former version. This is because it is required in order that the member before also including the deleted member may decode the code enciphered before deletion.

[0145] D. Go back and delete the member of deletion existing. The deleted member cannot decode the code enciphered before deletion, either. In this case, the pair of a new secret key and a public key is set to SG and PG of the group lock of a high version. Moreover, the value of F is "deleted." Therefore, the individual who received a high version does not delete a former version. This is because it is required in order that the member before removing the member deleted in the code enciphered before deletion may decode. However, when the individual who received is the member which cannot gain the secret key of a high version and which was case [the member] namely, deleted, it deletes. This is for the ability not decoding the member from which the code enciphered before deletion was also deleted. It is the thing of the character in which it cannot guarantee mathematically and deletion can be promoted as a system that this deleted member deletes the group lock of a former version.

[0146] When a group lock is changed, the value of F not only has a meaning, but it signs with the secret key for change of a former version. This is for trusting a high version automatically, when the former version is trusted, as mentioned above. When a group lock is changed, a required person is promptly supplied widely.

[0147] The group lock change flow shown in drawing 16 and drawing 17 is explained in full detail. The group lock

changed in Steps 901 and 902 is specified, and the kind of change is distinguished. Although either of the processings of an addition and deletion will be chosen in Step 902, when an addition and deletion occur simultaneously like exchange of a member, sequence is set up for every Memba and processing is performed for every Memba.

[0148] When change is the addition of a member in Step 902, it progresses to Step 903 and the public key of the group corresponding to the member added from an open lock list or an individual is chosen. Next, it is judged about whether it is necessary whether the addition from the present is sufficient as the addition of a step 904 smell lever, or to add going back to the past. That is, it is just determined whether ** will enable decode of the past code information. When judgment of Step 904 serves as an addition after "no", i.e., this time, "F" which the group public key PG, the group secret key SG, and a common key CG are generated at Step 905, and shows the direct previous-version treatment of a group lock at Step 906 is set up as it is required. This shows that the group lock of a new version and the group lock of the original earlier version live together. On the other hand, when judgment of Step 904 is "going back and adding", it progresses to Steps 907 and 908, SG of the group lock under present change, PG, and CG are set up as SG of the group lock changed as it was, PG, and CG, and F is set up with "needlessness." This shows that the group lock of the earlier version was completely transposed to the group lock of the new version. Next, at Step 909, the group secret key SG is enciphered with a common key CU, CG (SG) is generated, CG is further enciphered with the public key PMi of a member including an additional member, and the array of PMi (CG) which makes the label LMi corresponding to PMi an index is formed.

[0149] Next, the secret key of a change key is enciphered [Step 910] using the public key of the new right owner of change at generation of the pair of the secret key and public key of a change key, and Step 912 by a setup of the new right owner of change, and Step 911.

[0150] Furthermore, the signature by the change secret key to the data which was unified by renewal of version number V at Step 913, and was unified at unification of each data and Step 915 by Step 914 is performed, it is considered as the signature result Sig (SU), and the data which added the signature result further at Step 916 is unified. At Step 917, it signs by secret key SU' for change of a change previous version, and is referred to as Sig (SU'), the group lock changed at Step 918 is added to the trust lock list of makers, and the change procedure of a group lock is ended.

[0151] When change is deletion of a member in Step 902, the member which progresses to Step 919 and is deleted is chosen. Next, deletion of a step 920 smell lever is judged about whether it is necessary to go back to the past from the present. That is, it is just determined whether ** will enable decode of the past code information. When judgment of Step 920 serves as deletion after "no", i.e., this time, "F" which the group public key PG, the group secret key SG, and a common key CG are generated at Step 921, and shows the direct previous-version treatment of a group lock at Step 922 is set up as it is required. This shows that the group lock of a new version and the group lock of the original earlier version live together. On the other hand, when judgment of Step 920 is "going back and deleting", it progresses to Steps 923 and 924, SG of the group lock under present change, PG, and CG are set up as SG of the group lock changed as it was, PG, and CG, and F is set up with "deletion." Next, at Step 925, the group secret key SG is enciphered with a common key CG, a common key CG is further enciphered with the public key PMi of the ** member which deleted the deletion member, and the array of PMi (CG) which makes the label LMi corresponding to PMi an index is formed. It is the same as that of the case of an addition after Step 910 which is the following procedure.

[0152] [Example of mounting] Drawing 18 shows the example of a system which mounted the cipher system of the work example. In drawing 18 , two or more clients 20, the file server 30, and the directory server 40 are connected to the network 10. LAN is sufficient as a network 10 and WAN is sufficient as it. A file server 30 keeps files, such as a document. The directory server 40 is keeping the group lock. In such composition, the case where Client 20a keeps a document to a file server 30 is considered. KURAIN ** and 20a encipher a document with the public key which takes out a desired group lock from a directory server 40, and is contained there, and keep the enciphered document 50a to a file server 30. When Client 20b uses this document, Client 20b takes out a desired group lock from a directory server 40, acquires a secret key while it takes out Document 50a from a file server 30, and decodes an above-mentioned document with this secret key.

[0153] When Client 20a gives a signature to a document and keeps the document 50b with a signature to a file server 30 in this composition, Client 20a takes out a desired group lock from a directory server 40, acquires the secret key of a group lock, and signs with this secret key. Client 20b can verify the signature of a document using the public key of a group lock.

[0154] In addition, in drawing 18 , although the document of the file server 30 was the object of processing by a group lock, also when replacing with a file server 30 and using a mail server, same encryption and decoding processing, and a signature and verification processing are performed.
[0155] As mentioned above, although the work example of this invention was explained For example, generation of a double sign lock or change is the same, other components which may be performed in any and used in other public key cryptosystem of this, for example, various kinds of lock lists etc., such as encryption equipment, decode equipment, or equipment in the 3rd game of others, etc.
[0156] Moreover, in this work example, since it is a common key with the small (for example, 48-120 bits) number of bits, what is enciphered with a group member's secret key can generate a group lock at little quick cost, even when there are few amounts of processings of encryption and there are many members. Moreover, among a group lock, since the secret key of a group lock appears only once as a cipher enciphered with the common key, also when holding confidentiality, it is desirable.
[0157] In addition, since the secret key of a group lock is enciphered with the common key by the group lock of this work example, compared with the case where it enciphers with a public key, decode of a cipher is possible at low cost. Then, a secret key SG and SU are not directly enciphered with common keys CG and CU, but you may make it encipher the secret key (SG', SU') which deformed by CG and CU. The relation between the secret key which deformed, and the original secret key can be specified as follows.
[Mathematical formula 4] SG'=fG(SG)
SU'=fU(SU)
Function fG and fU are taken as the function which is not one way here. Therefore, inverse function fG-1 like the following formula and fU-1 exist in Function fG and fU.
[Mathematical formula 5] SG=fG -1(SG')
SU=fU -1(SU')
As long as an inverse function exists, what kind of thing is sufficient as the transformation function fG and fU. It can choose according to the grade of confidentiality.
[0158] When it does in this way, an aggressor is an inverse function fG, even if it decodes Ciphers CG (SG') and CU (SU') and acquires SG' and SU'. Since <SUP>-1 and fU-1 are not known, it is difficult to acquire a secret key SG and SU.
[0159] Moreover, you may use what attached what is called seed to the plaintext, and was enciphered instead of enciphering common keys CG and CU with a group member's public key, and making Cipher PMi (CG) and PMi (CU). This is as follows.
[Mathematical formula 6] PMi(CG+fP(PMi))
PMi(CU+fP(PMi))
In addition, fP is a function which inputs the public key to encipher and outputs a certain thing, for example, can use a hash function like MD5 and SHA1 (brand name). Since public keys differ for every Memba, they can differ in the candidate for encryption for every member, and as a result, they can raise safety integrity.
[0160] In the above-mentioned work example, since the common key is enciphered with each public key of a group member, the cipher of two or more CG appears in a group lock. Even in such a case, it is not necessary to give an aggressor a hint by seed.
[0161] In addition, although the secret key was enciphered with the common key and the common key was enciphered with the public key of the member in the above-mentioned work example, an encryption scheme which enciphers a secret key directly with the public key of a member is also considered. Such a scheme can also use the above seeds. That is, a group lock is constituted so that a secret key SG, PMi (SG) which enciphered SU with the public key PMi of the member, and PMi (SU) may be included (common keys CG and CU are not used). And also in this case, it replaces with PMi (SG) and PMi (SU), and PMi (SG+fP (PMi)) and PMi (SU+fP (PMi)) which put in seed can be included in a group lock.
[0162]
[Effect of the Invention] As explained above, it sets to the group type public key cryptosystem of this invention. The concept of a group is introduced into the public key cryptosystem which makes the conventional individual a unit. Execution of encryption processing of the plaintext by the arbitrary members belonging to a group and the decoding processing of code information was enabled by using a group combining the group public key, the group secret key, the individual public key, and secret key which were generated as a unit. By this composition, it made it possible to share code information on the basis of a check of being a member between the members in a group

between the inside of a group, and outside, maintaining advanced confidentiality. Moreover, the just encryption processing by a member and its check in a group were enabled by the electronic signature by the member belonging to a group.

[0163] furthermore, [the group type public key cryptosystem of this invention] On the occasion of change of the group lock to change of the member which constitutes a group, new generation and registration of a group public key and a group secret key of the pair were considered as the composition performed according to the change time of a member, and it had composition which can change a group lock flexibly to member change. Moreover, it set up to perform the signature for group lock change to the whole array of the element which constitutes a group lock, and the guarantee of change was offered the positive thing.

[0164] Moreover, since a common key with the comparatively small amount of data is enciphered with the cryptographic key of a member and he is trying to generate a group lock, there are few generation loads of a group lock and they end. Moreover, since the secret key of a group lock itself appears in a group lock only once in the mode enciphered with the common key, the hint of decode is not given to an aggressor.

[Brief Description of the Drawings]

[Drawing 1] It is the figure having shown the algorithm which determines the trust level of a compound lock.

[Drawing 2] It is the figure showing a determining-trust level of these other things algorithm from the trust level to a trust object, and the trust level to other things which the trust object has.

[Drawing 3] It is the block diagram showing the outline of the whole cipher system of this invention.

[Drawing 4] It is the figure showing the composition of the group lock of this invention.

[Drawing 5] It is the figure showing the composition of the open lock list of this invention.

[Drawing 6] It is the figure showing the composition of the secret lock list of this invention.

[Drawing 7] It is the figure showing the composition of the code of this invention.

[Drawing 8] It is the figure showing the group lock generation flow of this invention.

[Drawing 9] It is the figure showing the additional flow to the lock list of this invention.

[Drawing 10] It is the figure showing the availability judgment flow of the secret lock of this invention.

[Drawing 11] It is the figure showing the encryption flow of this invention.

[Drawing 12] It is the figure showing the decode possibility judgment flow of this invention.

[Drawing 13] It is the figure showing the acquisition flow of the secret key under secret lock list of this invention.

[Drawing 14] It is the figure showing the decode flow of this invention.

[Drawing 15] It is the figure showing the signature check flow of this invention.

[Drawing 16] It is the figure (the 1) showing the group lock change flow of this invention.

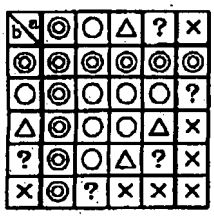
[Drawing 17] It is the figure (the 2) showing the group lock change flow of this invention.

[Drawing 18] It is the figure showing the system by which this invention is applied.

[Explanations of letters or numerals]

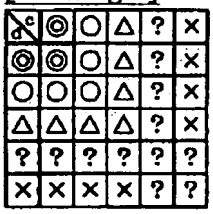
101 Individual
102 Plaintext
103 Code
104 Lock List
105 Individual Secret Key

[Drawing 1]



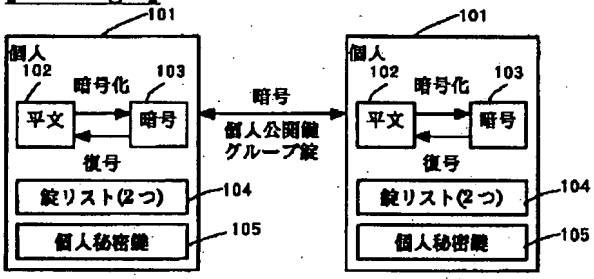
a：個人Aの信用レベル
b：個人Bの信用レベル

[Drawing 2]

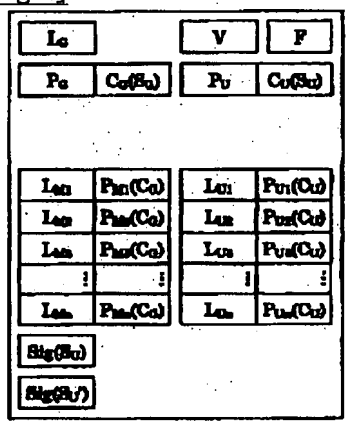


c：信用体に対する信用レベル
d：その信用体の他の信用体に対する信用レベル

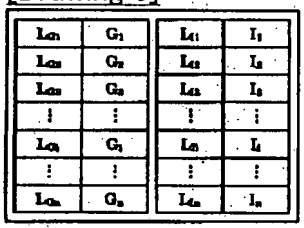
[Drawing 3]



[Drawing 4]



[Drawing 5]



G_i：信用しているグループ錠
L_{Gi}：グループ錠 G_i のラベル
I_i：信用している個人の公開鍵
L_{Ii}：個人の公開鍵 I_i に対応するラベル

[Drawing 6]

L_{G1}	G_1
L_{G2}	G_2
L_{G3}	G_3
⋮	⋮
L_{Gi}	G_i
⋮	⋮
L_{Gn}	G_n

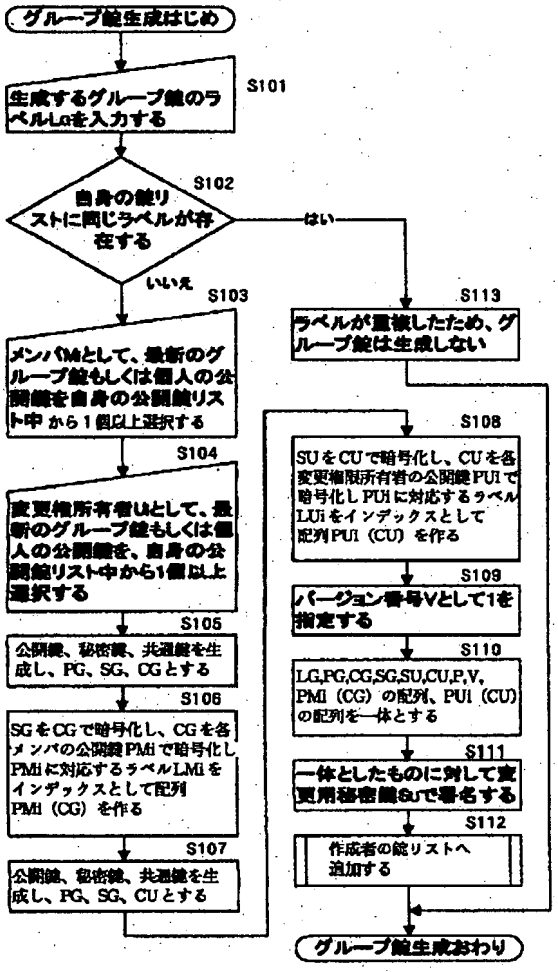
G_i: 秘密鍵が利用可能なグループ鍵

L_{Gi}: グループ鍵 G_i のラベル

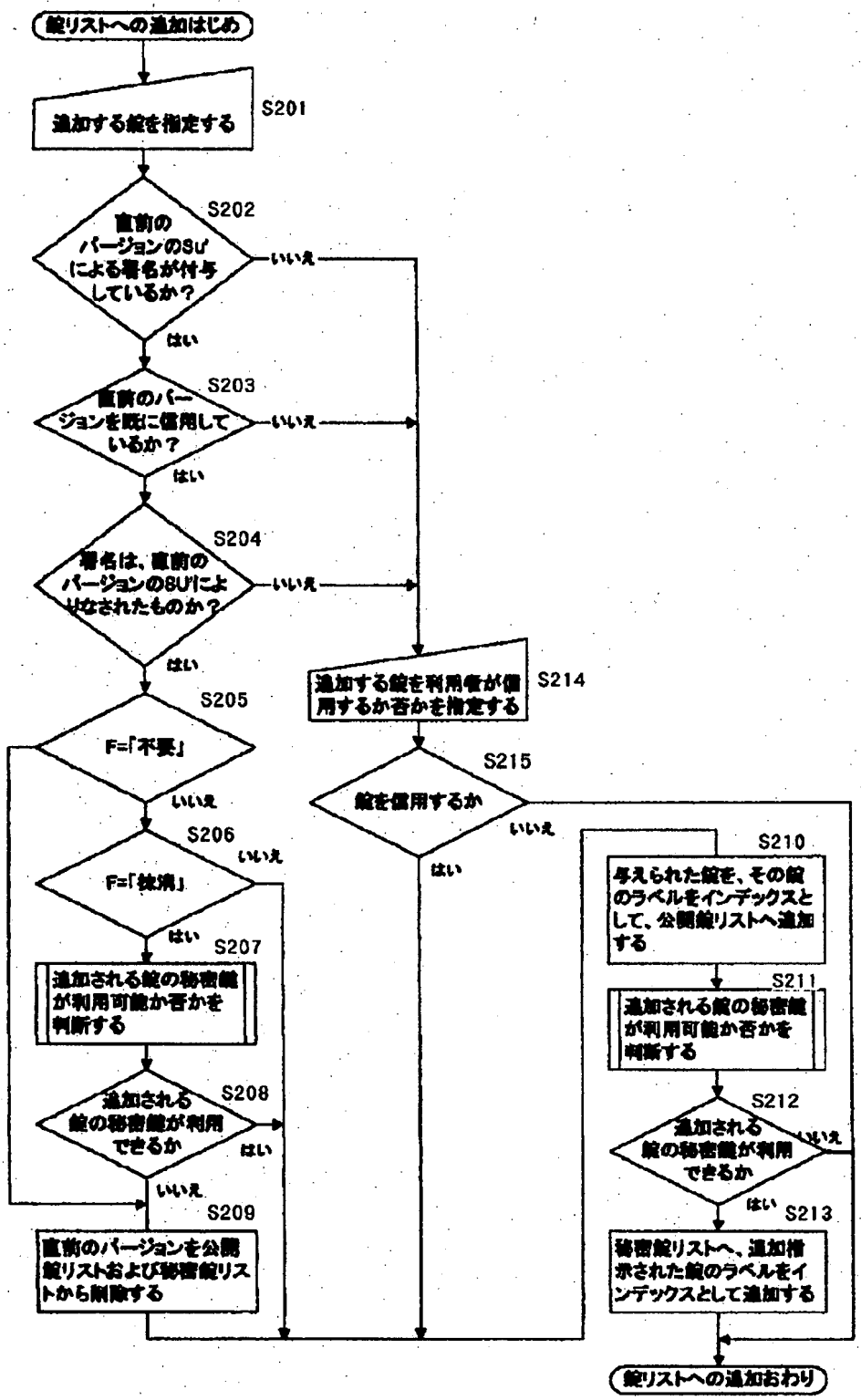
[Drawing 7]

L_1	$P_1(K)$
L_2	$P_2(K)$
L_3	$P_3(K)$
⋮	⋮
L_i	$P_i(K)$
⋮	⋮
L_n	$P_n(K)$
K(D)	
P	Sig(S)

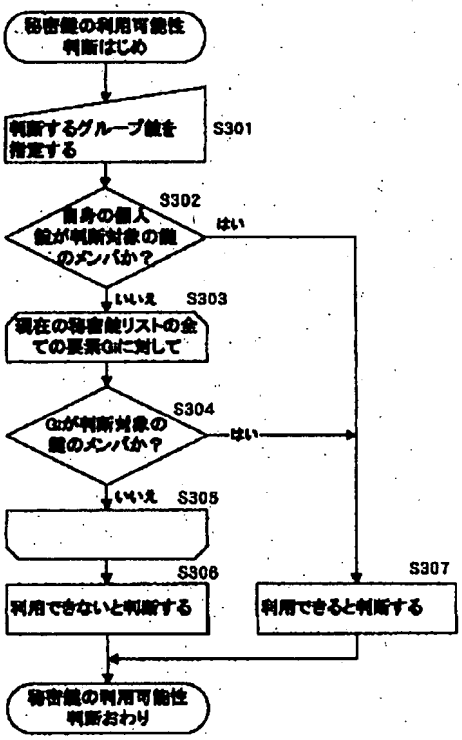
[Drawing 8]


グループ鍵生成はじめ
生成するグループ鍵のラベルLGを入力する
S101
自身の鍵リストに同じラベルが存在する
S102
はい
いいえ
S103
メンバMiとして、最新のグループ鍵もしくは個人の公開鍵を自身の公開鍵リスト中から1個以上選択する
S104
変更権所有者Uとして、最新のグループ鍵もしくは個人の公開鍵を、自身の公開鍵リスト中から1個以上選択する
S105
公開鍵、秘密鍵、共通鍵を生成し、PG、SG、CGとする
S106
SGをCGで暗号化し、CGを各メンバの公開鍵PMiで暗号化しPMiに対応するラベルLMiをインデックスとして配列PMi（CG）を作る
S107
公開鍵、秘密鍵、共通鍵を生成し、PG、SG、CUとする
S113
ラベルが重複したため、グループ鍵は生成しない
S108
SUをCUで暗号化し、CUを各変更権限所有者の公開鍵PUiで暗号化しPUiに対応するラベルLUiをインデックスとして配列PUi（CU）を作る
S109
バージョン番号Vとして1を指定する
S110
LG,PG,CG,SG,SU,CU,P,V,PMi（CG）の配列、PUi（CU）の配列を一体とする
S111
一体としたものに対して変更用秘密鍵SUで署名する
S112
作成者の鍵リストへ追加する
グループ鍵生成おわり

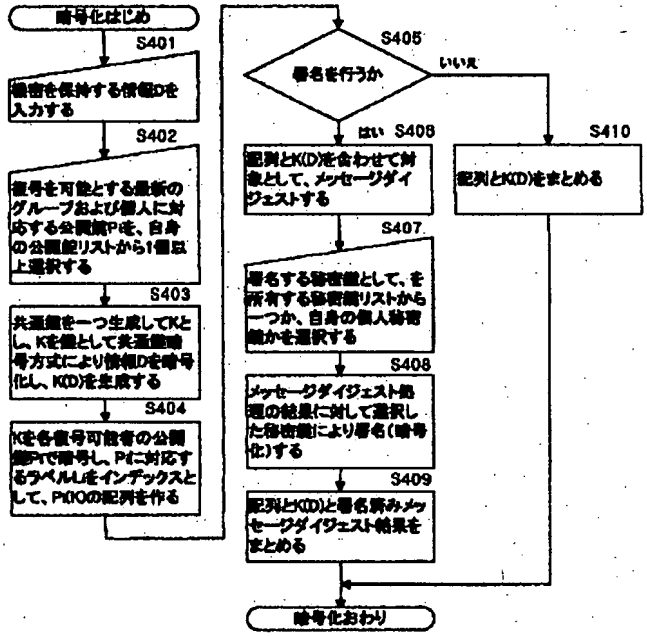
[Drawing 9]


鍵リストへの追加はじめ
追加する鍵を指定する
S201
直前のバージョンのSUによる署名が付与しているか？
S202
いいえ
はい
直前のバージョンを既に信用しているか？
S203
いいえ
はい
署名は、直前のバージョンのSUによりなされたものか？
S204
いいえ
はい
F=「不要」
S205
いいえ
F=「抹消」
S206
いいえ
はい
追加される鍵の秘密鍵が利用可能か否かを判断する
S207
追加される鍵の秘密鍵が利用できるか
S208
はい
いいえ
直前のバージョンを公開鍵リストおよび秘密鍵リストから削除する
S209
追加する鍵を利用者が信用するか否かを指定する
S214
鍵を信用するか
S215
いいえ
はい
与えられた鍵を、その鍵のラベルをインデックスとして、公開鍵リストへ追加する
S210
追加される鍵の秘密鍵が利用可能か否かを判断する
S211
追加される鍵の秘密鍵が利用できるか
S212
いいえ
はい
秘密鍵リストへ、追加指示された鍵のラベルをインデックスとして追加する
S213
鍵リストへの追加おわり

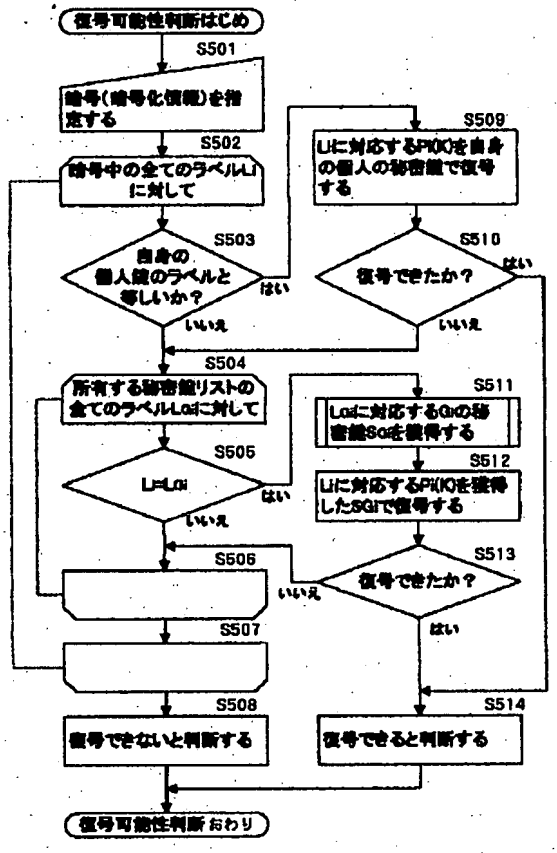
[Drawing 10]



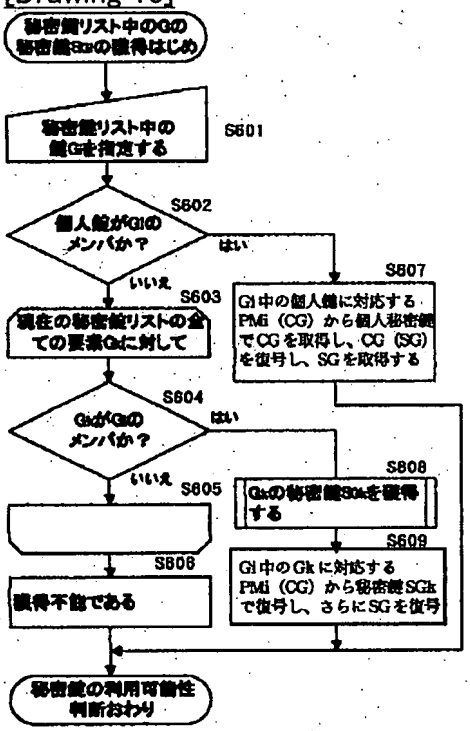
[Drawing 11]



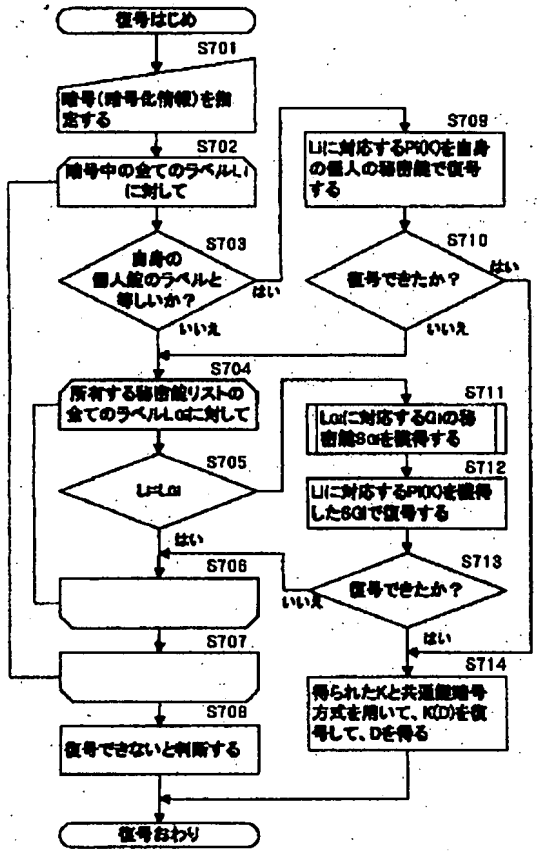
[Drawing 12]



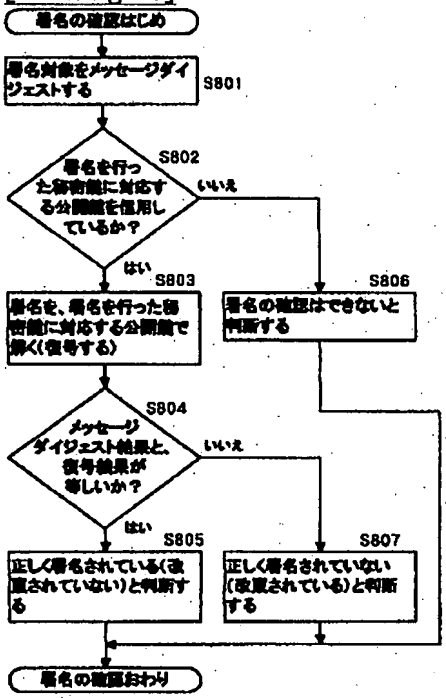
[Drawing 13]



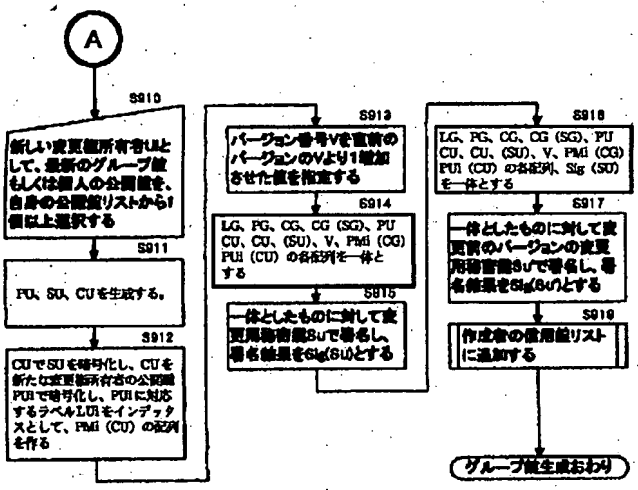
[Drawing 14]



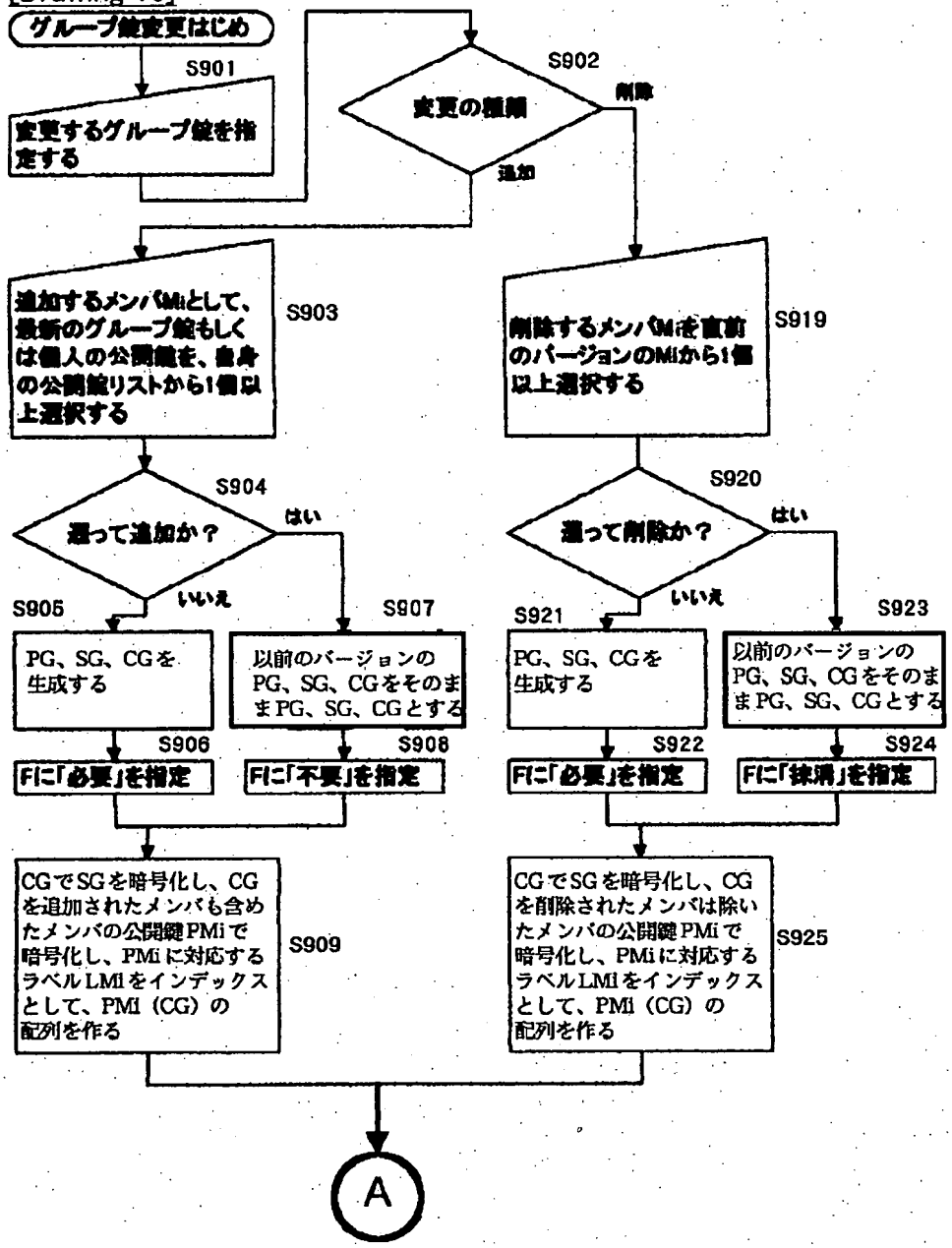
[Drawing 15]



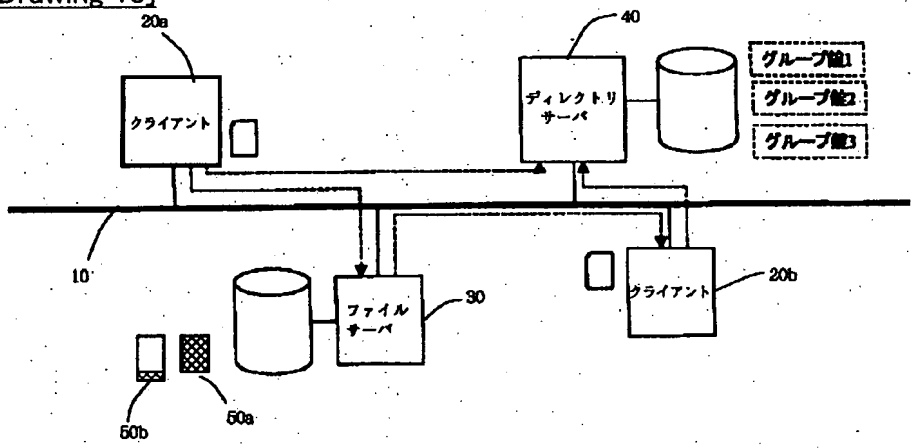
[Drawing 17]


A
S910
新しい変更権所有者Uとして、最新のグループ鍵もしくは個人の公開鍵を、自身の公開鍵リストから1個以上選択する
S911
PG、SG、CGを生成する。
S912
CGでSGを暗号化し、CGを新たな変更権所有者の公開鍵PUiで暗号化し、PUiに対応するラベルLiをインデックスとして、PMi（CG）の配列を作る
S913
バージョン番号Vを直前のバージョンのVより1増加させた値を指定する
S914
LG、PG、CG、CG（SG）、PU CU、CU、（SU）、V、PMi（CG）PUi（CU）の各配列を一体とする
S915
一体としたものに対して変更用秘密鍵SKuで署名し、署名結果をSig（SU）とする
S916
LG、PG、CG、CG（SG）、PU CU、CU、（SU）、V、PMi（CG）PUi（CU）の各配列、Sig（SU）を一体とする
S917
一体としたものに対して変更前のバージョンの変更用秘密鍵SKuで署名し、署名結果をSig（SU）とする
S918
作成前の使用鍵リストに追加する
グループ鍵生成おわり

[Drawing 16]


グループ鍵変更はじめ
S901
変更するグループ鍵を指定する
S902
変更の種類
削除
追加
S903
追加するメンバMiとして、最新のグループ鍵もしくは個人の公開鍵を、自身の公開鍵リストから1個以上選択する
S904
還って追加か？
はい
いいえ
S905
PG、SG、CGを生成する
S906
Fに「必要」を指定
S907
以前のバージョンのPG、SG、CGをそのままPG、SG、CGとする
S908
Fに「不要」を指定
S909
CGでSGを暗号化し、CGを追加されたメンバも含めたメンバの公開鍵PMiで暗号化し、PMiに対応するラベルLMiをインデックスとして、PMi（CG）の配列を作る
S919
削除するメンバMiを直前のバージョンのMiから1個以上選択する
S920
還って削除か？
はい
いいえ
S921
PG、SG、CGを生成する
S922
Fに「必要」を指定
S923
以前のバージョンのPG、SG、CGをそのままPG、SG、CGとする
S924
Fに「抹消」を指定
S925
CGでSGを暗号化し、CGを削除されたメンバは除いたメンバの公開鍵PMiで暗号化し、PMiに対応するラベルLMiをインデックスとして、PMi（CG）の配列を作る
A

[Drawing 18]



[Translation done.]